

The global isoperimetric methodology applied to Kneser's Theorem

Yahya O. Hamidoune*

February 1, 2008

Abstract

We give in the present work a new methodology that allows to give isoperimetric proofs, for Kneser's Theorem and Kemperman's structure Theory and most sophisticated results of this type. As an illustration we present a new proof of Kneser's Theorem.

1 Introduction

A basic tool in Additive Number Theory is the following generalization of the Cauchy-Davenport Theorem [2, 3] due to Kneser:

Theorem 1 (Kneser [18, 19, 20]) *Let G be an abelian group and let $A, B \subset G$ be finite subsets such that $|A + B| \leq |A| + |B| - 2$. Then $A + B$ is periodic.*

The above compact form of Kneser's Theorem implies easily the following popular form of this theorem:

Corollary 2 (Kneser [18, 19, 20]) *Let G be an abelian group and let $A, B \subset G$ be finite subsets. Then $|A + B| \geq |A + H| + |B + H| - |H|$, where H is the period of $A + B$.*

Proofs of this result based on the additive local transformations introduced by Cauchy and Davenport [2, 3] are contained in [18, 19, 20].

Recently the author introduced the isoperimetric method allowing to derive additive inequalities from global properties of the fragments and atoms (subsets where the objective function $|A + B| - |A|$ achieves its minimal non trivial value).

This method can be applied to abstract graphs and non abelian groups and have implications that could not be derived using the local transformations. However in the abelian case, it was not clear how to derive the Kneser-Kemperman's Theory from the isoperimetric method.

*Université Pierre et Marie Curie, Paris hamidoune@math.jussieu.fr

Very recently Balandraud introduced some isoperimetric objects and proposed a proof, requiring several pages, of Kneser's Theorem using as a first step our result that the 1-atom containing 0 is a subgroup.

The purpose of the present paper is not to give a short proof of Kneser's Theorem. Each of the direct proofs contained in [18, 20] is quite short and requires around three pages. However the present proof gives more light on the isoperimetric nature of Kneser's Theorem and shows that it follows from the fundamental property of the 1-atoms.

More interesting than this new proof is the methodology which could be applied in the following contexts:

- It will be used in a coming paper to Kemperman's structure Theorem [16] and its critical pair Theorem proved recently by Gryniewicz [5], producing considerable simplifications.
- Quite likely this method could be applied to solve the open question concerning the description for subsets A, B with $|A + B| = |A| + |B| + m$, for some values of $m > 0$.
- This method is purely combinatorial and could be adapted to non abelian groups. Indeed the major part of the arguments of this paper holds for non abelian groups.

2 Terminology and preliminaries

2.1 Groups

Let G denotes an abelian group. The subgroup generated by a subset S will be denoted by $\langle S \rangle$. Let A, B be subsets of G . The *Minkowski sum* is defined as

$$A + B = \{x + y : x \in A \text{ and } y \in B\}.$$

For an element $x \in G$, we write $r_{A,B}(x) = |(x - B) \cap A|$. Notice that $r_{A,B}(x)$ is the number of distinct representations of x as a sum of an element of A and an element of B .

We use the following well known fact:

Lemma 3 [19] *Let G be a finite group and let A, B be subsets such that $|A| + |B| \geq |G| + t$. Then $r_{A,B}(x) \geq t$.*

Let H be a subgroup. A partition $A = \bigcup_{i \in I} A_i$, where A_i is the nonempty intersection of some H -coset with A will be called a *H -decomposition* of A .

2.2 The strong isoperimetric property

Let V be a set and let $E \subset V \times V$. The relation $\Gamma = (V, E)$ will be called a *graph*. An element of V will be called a *point* or a *vertex*. The graph Γ is said to be *reflexive* if $(x, x) \in E$, for all x . We shall write

$$\partial(X) = \Gamma(X) \setminus X.$$

A *path* of Γ from x_1 to x_k is a sequence $\mu = [x_1, \dots, x_k]$ of pairwise distinct points (where $k \geq 1$) such that $(x_i, x_{i+1}) \in E$, for all $1 \leq i \leq k-1$. The set of points of μ is by definition $P(\mu) = \{x_1, \dots, x_k\}$. Our paths are called elementary paths in some Graph Theory books.

A family μ_1, \dots, μ_k of paths from x to y will be called *openly disjoint* if $P(\mu_i) \cap P(\mu_j) = \{x, y\}$ for all i, j with $i \neq j$.

Let $\Gamma = (V, E)$ be a locally finite graph with $|V| \geq 1$. The *1-connectivity* of Γ is defined as

$$\kappa_1(\Gamma) = \min\{|\partial(X)| : \infty > |X| \geq 1 \text{ and } |X \cup \Gamma(X)| \leq |V| - 1\}, \quad (1)$$

where $\min \emptyset = |V| - 1$.

Let G be a group, written additively, and let S be a subset of G . The graph (G, E) , where $E = \{(x, y) : -x + y \in S\}$ is called a *Cayley graph*. It will be denoted by $\text{Cay}(G, S)$.

Let $\Gamma = \text{Cay}(G, S)$ and let $F \subset G$. Clearly $\Gamma(F) = F + S$.

A general formalism, including the most recent terminology of the isoperimetric method, may be found in the recent paper [14].

Let x, y be elements of V . We shall say that y is $(k-1)$ -*nonseparable* to x in Γ if $|\partial(A)| \geq k$, for every subset A with $x \in A$ and $y \notin \Gamma(A)$.

We shall formulate Menger's Theorem (the general form of this result is due to Dirac) which is a basic fact from Graph Theory. It has applications in Additive number Theory [19, 20].

Theorem 4 (*Dirac-Menger*)[19, 20]

Let $\Gamma = (V, E)$ be a finite reflexive graph. Let k be a nonnegative integer. Let $x, y \in V$ such that y is $(k-1)$ -nonseparable from x , and $(x, y) \notin E$. Then there are k openly disjoint paths from x to y .

One may formulate Menger's Theorem for non reflexive graphs. Such a formulation is slightly more complicated and follows easily from the reflexive case. We shall give an isoperimetric short proof of this result in the appendix.

We need the following consequence of Menger's Theorem:

Proposition 5 *Let Γ be a locally finite reflexive graph and let k be a nonnegative integer with $k \leq \kappa_1$. Let X a finite subset of V such that $\min(|V| - |X|, |X|) \geq k$. There are pairwise distinct elements $x_1, x_2, \dots, x_k \in X$ and pairwise distinct elements $y_1, y_2, \dots, y_k \notin X$ such that*

- $(x_1, y_1), \dots, (x_k, y_k) \in E$,
- $|X \cup \{y_1, \dots, y_k\}| = |X| + k$,

Proof. By the definition of κ_1 , we have $|\partial(Y)| \geq \min(|V| - |Y|, |Y|) \geq k$, for every $Y \subset V$. Let $\Phi = (\Gamma(X), E')$ be the restriction of Γ to $\Gamma(X)$ (observe that $X \subset \Gamma(X)$). Choose two elements $a, b \notin V$. Let Ψ be the reflexive graph obtained by connecting a to $X \cup \{a\}$ and $\partial(X) \cup \{b\}$ to

b. We shall show that b is $(k-1)$ -nonseparable from a in Ψ . Take $a \in T$ such that $b \notin \Psi(T)$. Then clearly $T \subset X \cup \{a\}$. Assume first $T = \{a\}$. Then $|\Psi(T)| - |T| = |X \cup \{a\}| - 1 \geq k$. Assume now $T \cap X \neq \emptyset$. We have $\Psi(T) = X \cup \{a\} \cup \Gamma(T \cap X)$. Therefore

$$|\Psi(T)| \geq 1 + |X| + |\Gamma(T \cap X) \setminus X| \geq 1 + |X| + (|T \cap X| + k - |X|) > k.$$

By Menger's Theorem there are P_1, \dots, P_k openly disjoint paths from a to b . Choose x_i as the last point of the path P_i belonging to X and let y_i the successor of x_i on the path P_i . This choice satisfies the requirements of the proposition. ■

We call the property given in Proposition 5 the *strong isoperimetric property*.

3 Isoperimetric preliminaries

The isoperimetric method is usually developed in the context of graphs. We need in the present work only the special case of Cayley graphs on abelian groups that we shall identify with group subsets.

Throughout all this section, S denotes a finite generating subset of an abelian group G , with $0 \in S$.

For a subset X , we put $\partial_S(X) = (X + S) \setminus X$ and $X^S = G \setminus (X + S)$.

Lemma 6 [1, 14] *Let X be a subset of G . Then $(X^S)^{-S} + S = X + S$.*

The last lemma is proved in Balandraud [1] and generalized in [14].

The 1-connectivity of S is defined as $\kappa_1(S) = \kappa_1(\text{Cay}(G, S))$. By the definitions we have

$$\kappa_1(S) = \min\{|\partial(X)| : \infty > |X| \geq 1 \text{ and } |X + S| \leq |G| - 1\}, \quad (2)$$

where $\min \emptyset = |G| - 1$.

A finite subset X of G such that $|X| \geq 1$, $|G \setminus (X + S)| \geq 1$ and $|\partial(X)| = \kappa_1(S)$ is called a 1-fragment of S . A 1-fragment with minimum cardinality is called a 1-atom. The cardinality of a 1-atom of S will be denoted by $\alpha_1(S)$.

If $S = G$, a 1-fragment (resp. 1-atom) is just a set with cardinality 1.

These notions, are particular cases some concepts in [7, 10, 11, 13, 14]. The reader may find all basic facts from the isoperimetric method in the recent paper [14].

Notice that $\kappa_1(S)$ is the maximal integer j such that for every finite nonempty subset $X \subset G$

$$|X + S| \geq \min(|G|, |X| + j). \quad (3)$$

Formulae (3) is an immediate consequence of the definitions. We shall call (3) the *isoperimetric inequality*. The reader may use the conclusion of this lemma as a definition of $\kappa_1(S)$.

Since $|\partial(\{0\})| \leq \kappa_1$, we have:

$$\kappa_1(S) \leq |S| - 1. \quad (4)$$

The basic intersection theorem is the following:

Theorem 7 [11, 14]

Let S be a generating subset of an abelian group G with $0 \in S$. Let A be a 1-atom and let F be a 1-fragment such that $|A \cap F| \geq 1$. Then $A \subset F$. In particular distinct 1-atoms are disjoint.

The structure of 1-atoms is the following:

Proposition 8 [9, 8, 12]

Let S be a generating subset of an abelian group G with $0 \in S$. Let H be a 1-atom of S with $0 \in H$. Then H is a subgroup. Moreover

$$\kappa_1(S) \geq \frac{|S|}{2}, \quad (5)$$

Proof. Take $x \in H$. Since $x \in (H+x) \cap H$ and since $H+x$ is a 1-atom, we have $H+x = H$ by Theorem 7. Therefore H is a subgroup. Since S generates G , we have $|H+S| \geq 2|H|$, and hence $\kappa_1(S) = |H+S| - |H| \geq \frac{|S+H|}{2} \geq \frac{|S|}{2}$. ■

Let us formulate two corollaries:

Corollary 9 [9, 8, 12] *Let S be a nonempty subset of an abelian group G . Let Q be the subgroup generated by $S - S$. Let T be a subset of G such that $T + Q \neq T$. Then*

$$|T + S| \geq |T| + \frac{|S|}{2}, \quad (6)$$

Proof. Take an element a of S and put $X = S - a$. Since $X - X = S - S$, X generates Q . Take a Q -decomposition $T = \bigcup_{i \in J} T_i$. Since $T + Q \neq T$, there is a j with $T_j + S \neq T_j$. Take $b \in T_j$, we have using by (5):

$$\begin{aligned} |T + S| &= \sum_{i \neq j} |T_i + S| + |T_j + S| = |T| - |T_j| + |T_j - b_j + S - a| \\ &= |T| - |T_j| + (|T_j| + \frac{|S|}{2}) = |T| + \frac{|S|}{2}. \end{aligned}$$

■

Corollary 10 *Let S and T be nonempty subsets of an abelian group G such that $|T + S| \leq |T| + |S| - m$ and $0 \in S$, for some $m \geq 0$.*

Then there are $a \in G$ and $T' \subset a + \langle S \rangle$, such that $(T \setminus T') + \langle S \rangle = T \setminus T'$ and $|T' + S| \leq |T'| + |S| - m$.

Proof. Decompose $T = \bigcup_{i \in U} T_i$ modulo $\langle S \rangle$. By (5), $\kappa_1(S) \geq \frac{|S|}{2}$. Put $V = \{i \in U : |T_i + S| < |\langle S \rangle|\}$. By (3) we have

$$\begin{aligned} |T + S| &\geq \sum_{i \notin V} |T_i + S| + \sum_{i \in V} |T_i + S| \\ &\geq (|U| - |V|)|\langle S \rangle| + \sum_{i \in V} |T_i| + |V| \frac{|S|}{2} \geq |T| + |V| \frac{|S|}{2}. \end{aligned}$$

It follows that $|V| \leq 1$. The result holds clearly if $V = \emptyset$, since $T + S = T + S + \langle S \rangle$ in this case. Suppose that $V = \{\omega\}$. We have clearly $|T_\omega + S| \leq |T_\omega| + |S| - m$.

■

3.1 Fragments in quotient groups

We need the following lemma:

Lemma 11 *Let S be a finite generating subset of an abelian group G with $0 \in S$. Let H be a subgroup which is a 1-fragment and let $\phi : G \mapsto G/H$ be the canonical morphism. Then*

$$\kappa_1(\phi(S)) = |\phi(S)| - 1. \quad (7)$$

Proof.

Put $|\phi(S)| = u + 1$. Since $|G| > |H + S|$, we have $\phi(S) \neq G/H$, and hence $\phi(S)$ is 1-separable.

Let $X \subset G/H$, be such that $X + \phi(S) \neq G/H$. Clearly $\phi^{-1}(X) + S \neq G$. Then $|\phi^{-1}(X) + S| \geq |\phi^{-1}(X)| + \kappa_1(S) = |\phi^{-1}(X)| + u|H|$.

It follows that $|X + \phi(S)||H| \geq |X||H| + u|H|$. Hence $\kappa_1(\phi(S)) \geq u = |\phi(S)| - 1$. ■

4 An isoperimetric proof of Kneser's Theorem

Proof of Theorem 1:

Without loss of generality we may assume that $0 \in S$ and $|S| \leq |T|$. The proof is by induction on $|S| + |T|$, the result being obvious for $|S| + |T|$ small.

Claim 1 If $T \not\subset \langle S \rangle$, then the result holds.

Proof. By Corollary 10, there are $a \in G$ and $T' \subset a + \langle S \rangle$, such that $(T \setminus T') + \langle S \rangle = T \setminus T'$. and $|T' + S| \leq |T'| + |S| - 2$. Without loss of generality we may assume that $0 \in T'$. By the induction hypothesis there is a non zero subgroup N of $\langle S \rangle$, such that $T' + S + N = T' + S$. It follows that $T + S + N = T + S$. ■

By Claim 1, we may assume without loss of generality that

$$G = \langle S \rangle.$$

Assume first $|G| - |T + S| = |T^S| < |T|$. Then G is finite. By the definition $(T^S - S) \cap T = \emptyset$. Therefore $|T^S - S| \leq |G| - |T| = |G| - |S + T| + |S + T| - |T| \leq |T^S| + |S| - 2$. Since $|T^S| + |S| < |T| + |S|$, we have by the induction hypothesis, $T^S - S = T^S - S + N$, for some non zero subgroup N . Then $(G \setminus (T^S - S)) = T^{S^{-S}}$ is N -periodic, and hence by Lemma 6 $T + S = T^{S^{-S}} + S$ is N -periodic. So we may assume

$$|S| \leq |T| \leq |T^S|. \quad (8)$$

We prove first the bound

$$|S + T| \leq \frac{2|G| - 2}{3}. \quad (9)$$

By the assumption $|T^S| = |G| - |T + S| \geq |T| \geq |S|$, we have

$$\begin{aligned} 3|S + T| &\leq 2|S + T| + |S| + |T| - 2 \\ &\leq |G| - |S| + |G| - |T| + |S| + |T| - 2 = 2|G| - 2, \end{aligned}$$

which proves (9).

Let H be a 1-atom S and let $\phi : G \mapsto G/H$ denotes the canonical morphism. Put $|\phi(S)| = u+1$ and $|\phi(T)| = t+1$.

Take a H -decomposition $S = \bigcup_{0 \leq i \leq u} S_i$ such that $|S_0| \geq \dots \geq |S_u|$. By the definition of a 1-atom we have $u|H| = |H + S| - |H| = \kappa_1 \leq |S| - 2$. It follows that for all $u \geq j \geq 0$

$$|S_{u-j}| + \dots + |S_u| \geq j|H| + 2 \quad (10)$$

It follows that $|S_0| \geq \frac{|H|+2}{2}$. In particular S_0 generates H .

We shall use this fact in the application of the isoperimetric inequality.

Take a H -decomposition $T = \bigcup_{0 \leq i \leq t} T_i$.

By (7), $\kappa_1(\phi(S)) = |\phi(S)| - 1 = u$. Put $\ell = \min(q - t - 1, u)$.

By Proposition 5 applied to $\phi(S)$ and $\phi(T)$, there is a subset $J \subset [0, t]$ with cardinality ℓ and a family $\{mi; i \in J\}$ of integers in $[1, u]$ such that $T + S$ contains the H -decomposition $(\bigcup_{0 \leq i \leq t} T_i + S_0) \cup (\bigcup_{i \in J} T_i + S_{mi}) \cup R$,

where $R = (S + T) \setminus ((\bigcup_{i \in J} T_i + S_{mi} + H) \cup (\bigcup_{0 \leq i \leq t} T_i + H))$.

We shall choose such a J in order to maximize $|J \cap P|$. We shall write $E_i = (S + T) \cap (T_i + H)$, for every $i \in [0, t]$. Also we write $E_{mi} = (S + T) \cap (T_i + S_{mi} + H)$, for every $i \in J$.

We put also $W = \{i \in [0, t] : |E_i| < |H|\}$, and $P = [0, t] \setminus W$. We write also $q = \frac{|G|}{|H|}$.

Since $|T| \geq |S|$ we have $|T + H| \geq |S| > \kappa_1(S) = u|H|$. It follows that $t + 1 = |\phi(T)| \geq u + 1$. Then $t + 1 - |J| > 0$. In particular $I \neq \emptyset$, where $I = [0, t] \setminus J$.

Let X be a subset of I and let Y be a subset of J . We have

$$\begin{aligned} |S + T| - |R| &\geq \sum_{i \in X \cup Y} |E_i| + \sum_{i \in I \setminus X \cup J \setminus Y} |T_i + S_0| + \sum_{i \in J \setminus Y} |T_i + S_{mi}| + \sum_{i \in Y} |E_{mi}| \\ &\geq \sum_{i \in X \cup Y} |E_i| + \sum_{i \in I \setminus X \cup J \setminus Y} |T_i| + (u - |Y|)|S_0| + \sum_{i \in Y} |E_{mi}| \end{aligned} \quad (11)$$

$$\geq \sum_{i \in X \cup Y} |E_i| + \sum_{i \in I \setminus X \cup J \setminus Y} |T_i| + (u - |Y|)|S_0| + |Y||S_u| \quad (12)$$

Put $F = \{i \in I \cap P : (T_i + S) \cap (\bigcup_{i \in W} T_i + H) \neq \emptyset\}$.

We shall use the following obvious facts: For all $i \in W$, we have by (5), $|E_i| \geq |T_i + S_0| \geq |T_i| + \kappa_1(S_0) \geq |T_i| + \frac{|S_0|}{2}$. For every $i \in F$, $T_i + S_{ri} \subset T_j + H$ for some $1 \leq ri \leq u$ and some $j \in W$. Hence we have $|T_i| + |S_u| \leq |T_i| + |S_{ri}| \leq |H| = |E_i|$, by Lemma 3.

Let U be a subset of $W \cap J$. Put $X = I$ and $Y = U$. By (12), we have

$$|S + T| - |R| \geq \sum_{i \in U \cup (W \cap I) \cup (P \cap I)} |E_i| + \sum_{i \in J \setminus U} |T_i| + (u - |U|)|S_0| + |U||S_u| \quad (13)$$

$$\begin{aligned} &\geq \sum_{i \in (P \cap I) \setminus F} |T_i| + \sum_{i \in F} (|T_i| + |S_u|) + \sum_{i \in (W \cap I) \cup U} (|T_i| + \frac{|S_0|}{2}) + |J \setminus U||S_0| + |U||S_u| \\ &\geq |T| + |J \setminus U||S_0| + (|U| + |F|)|S_u| + |(W \cap I) \cup U| \frac{|S_0|}{2}. \end{aligned} \quad (14)$$

Claim 2 $q \geq |\phi(S)| + |\phi(T)| - 1$, and hence $\ell = u$.

Proof. The proof is by contradiction. Suppose that $q < |\phi(S)| + |\phi(T)| - 1$.

Assume first $u \geq 2$. By Lemma 3, there are two distinct values of the pair (s, t) such that $T_s + S_t \subset E_{mi}$, for every $i \in J$. In particular $|E_{mi}| \geq |S_{u-1}|$, for every $i \in J$. Also $|E_i| \geq |S_0|$, for every $i \in [0, t]$.

Observe that $2t > t + u \geq q$. We have using (10)

$2|S_0| \geq |S_0| + |S_{u-1}| \geq \frac{2}{3}(|S_u| + |S_{u-1}| + |S_{u-2}|) > \frac{4|H|}{3}$. By (12), applied with $X = I$ and $Y = J$, we have

$$\begin{aligned} |S + T| &\geq \sum_{0 \leq i \leq t} |S_0| + \sum_{i \in J} |S_{u-1}| = (t + 1)|S_0| + (q - t - 1)|S_{u-1}| \\ &= (2t + 2 - q)|S_0| + (q - t - 1)(|S_0| + |S_{u-1}|) \\ &> (2t + 2 - q) \frac{2|H|}{3} + \frac{4|H|(q - t - 1)}{3} = \frac{2|G|}{3}, \end{aligned}$$

contradicting (9).

Assume now $u = 1$.

From the inequality $|T + S| \leq |T| + |S| - 2$, we see that $\kappa_1(S) \leq |S| - 2$. Therefore we have by (9), $\frac{2|G|}{3} > |T + S| \geq |T| + \kappa_1(S) \geq |S| + |H| > 2|H|$, and hence

$$q \geq 4.$$

We have $(t + 1) + (u + 1) - 1 < |\phi(S + T)| \leq q$. Then $t + 1 = q$. Hence $\ell = |J| = 0$. We have $|W| \geq 1$, since otherwise $G = T + H \subset S + T$. We have $|W| \leq 3$, by (14) applied with $U = \emptyset$. Therefore $|P| \geq t + 1 - 3 \geq 4 - 3 = 1$. There is clearly $i \in P$ with $T_i + S_1 \subset T_j + H$ for some $j \in W$, and hence $|F| \geq 1$. By (14) applied with $U = \emptyset$, $|T + S| \geq |T| + |W| \frac{|S_0|}{2} + |S_1|$, and hence $|W| \leq 1$. It follows that $|S + T| \geq |G| - |H| = |G| - \frac{|G|}{q} \geq \frac{3|G|}{4}$, contradicting (9). ■

We must have $R = \emptyset$, since otherwise by (14) applied with $U = \emptyset$, $|S + T| - |R| \geq |S + T| - |S_u| |\phi(R)| \geq |T| + u|S_0| + |S_u| \geq |T| + |S|$, a contradiction. In particular

$$|\phi(S + T)| = |\phi(S)| + |\phi(T)| - 1. \quad (15)$$

Claim 3. $J \cap P \neq \emptyset$.

Proof. Suppose the contrary and take $k \in J \cap W$. Put $U = \{k\}$. By (14),

$$|S| + |T| > |S + T| \geq |T| + (u - 1)|S_0| + |S_u| + (|W \cap I| + 1) \frac{|S_0|}{2}.$$

It follows that $I \subset P$. Since S generates G , we have $|\bigcup_{i \in I} T_i + H + S| > |\bigcup_{i \in I} T_i + H|$.

We must have $(\bigcup_{i \in I} T_i + H + S) \cap (\bigcup_{i \in J} E_{mi} + H) = \emptyset$, since otherwise by replacing a suitable element of J with some $p \in I$, we may increase strictly $|J \cap P|$, observing that $I \subset P$.

By (15), there are $i \in I$, $j \in J$ and $p \in [1, u]$ such that $T_i + S_p$ is congruent $T_j + S_{mj}$. It follows that $F \neq \emptyset$.

By (14) applied with $U = \emptyset$,

$$|S + T| \geq |T| + u|S_0| + |S_u| \geq |T| + |S|,$$

a contradiction proving the claim. ■

Take $r \in J$ with $|E_r| = |H|$. Such an r exists by Claim 3.

Claim 4 $T_i + H + S_j = T_i + S_j$, for all $0 \leq j \leq u - 1$.

Proof. By Lemma 3, it would be enough to show the following:

$$|T_k| + |S_{u-1}| > |H|, \quad (16)$$

for every $k \in [0, t]$. Suppose the contrary.

Notice that $|E_{mr}| \geq \max(|T_r|, |S_u|)$ and that $|E_k| \geq |S_0|$. Also $|T_k| + |S_{u-1}| \leq |H| = |E_{mr}|$ by our hypothesis. We shall use these inequalities and (11) with $X = \{k, r\} \cap I$ and $Y = \{k, r\} \cap J$.

By (11) we have for $k \neq r$,

$$\begin{aligned} |S + T| &\geq |T| - |T_k| - |T_r| + (u - |X|)|S_0| + |T_k| + |S_{u-1}| + |S_0| + |T_r| + |Y||S_u| \\ &\geq |T| + (u - 1)|S_0| + |S_{u-1}| + |S_u| \geq |T| + |S|, \end{aligned}$$

leading a contradiction. If $k = r$ the contradiction comes more easily. ■

Put $D = \{i \in J : T_i + S_{mi} + H \not\subset S + T\}$ and $C = (T + H) \cup \bigcup_{i \in J \setminus D} (T_i + S_{mi} + H) \cup \bigcup_{i \in D} (T_i + S_u)$.

We shall show that

$$T + S = C. \quad (17)$$

By (15), we have $|\phi(C)| = t + 1 + u = |\phi(S + T)|$. By the definition of D and by Claim 4, $C \setminus (\bigcup_{i \in D} (T_i + S_u))$ is H -periodic subset of $S + T$. It remains to show that the traces of $S + T$ and C coincide on the cosets represented by elements in $\bigcup_{i \in D} (T_i + S_u)$. Take $i \in D$. It follows by Claim 4 that $mi = u$. We can not have $T_l + S_j \equiv T_i + S_u \pmod{H}$ for some $j \neq u$, since otherwise by Claim 4 $T_l + H + S_j = T_l + S_j$, and $i \notin D$, a contradiction. The proof of (17) is complete.

Let $Q = \langle S_u - S_u \rangle$. By (10) we have $|Q| \geq |S_u| \geq 2$. Put $D' = \{i \in D : T_i + S_{mi} + Q \neq T_i + S_{mi}\}$. By (6) we have, $|T_i + S_u| \geq |T_i| + \frac{|S_u|}{2}$.

By the definition of D' and since $Q \subset H$, we have

have using (11), applied with $X = \emptyset$ and $Y = D'$

$$|S + T| \geq |T| - \sum_{i \in D'} |T_i| + \sum_{i \in D'} |E_{mi}| + u|S_0| \geq |T| + u|S_0| + |D'| \frac{|S_u|}{2}.$$

Clearly $T + S + Q = T + S$ if $D' = \emptyset$. Suppose $D' \neq \emptyset$. We must have $|D'| \leq 1$, since otherwise $|S + T| \geq |T| + u|H| + |S_u| \geq |T| + |S|$, a contradiction. Then $|D'| = 1$. Put $D' = \{o\}$. Take $x_o \in T_o$. We have $|T_o - x_o + S_u - a_u| = |T_o + S_u| \leq |T_o| + |S_u| - 2$ since otherwise $|S + T| \geq |S| + |T| - 1$. By the induction hypothesis there is a nonzero subgroup N of Q , with $T_o - x_o + s_u - a_u + N = T_o - x_o + s_u - a_u$. It follows that $T_o + S_u + N = T_o + S_u$. We have clearly $S + T + N = S + T$.

■

5 Appendix : An isoperimetric proof of Menger's Theorem

We present here an isoperimetric proof of Menger's Theorem. Let $E \subset V \times V$ and let $\Gamma = (V, E)$ be a reflexive graph. For a subset X of V , we put $X^\perp = V \setminus \Gamma(X)$. Let x, y be elements of V . The graph Γ will be called (x, y) - k -critical if y is $(k - 1)$ -nonseparable from x in Γ , and if this property is destroyed by the deletion of every arc (u, v) with $u \neq v$.

A subset A with $x \in A$ and $y \notin \Gamma(A)$ and $|\partial(A)| = k$ will be called a k -part with respect to $(x, y; \Gamma)$.

The reference to (x, y) will be omitted.

Lemma 12 *Assume that $\Gamma = (V, E)$ is k -critical and let $(u, v) \in E$ be an arc with $u \neq v$. Then Γ has k -part F with $u \in F$ and $v \in \partial(F)$.*

Proof.

Consider the graph $\Psi = (V, E \setminus \{(u, v)\})$. There is an F with $x \in F$ and $y \notin \Psi(F)$ such that $|\partial_\Psi(F)| < k$. This forces that $u \in F$ and that $v \in \partial(F)$, since otherwise $\partial_\Psi(F) = \partial_\Gamma(F)$.

Since $\partial_\Psi(F) \cup \{v\} \supset \partial_\Gamma(F)$, we have $|\partial_\Gamma(F)| \leq k$. We must have $|\partial_\Gamma(F)| = k$, since y is $(k-1)$ -nonseparable from x in Γ . This shows that F is a k -part.

■

Lemma 13 *Let F be a k -part with respect to $(x, y; \Gamma)$. Then F^\wedge is a k -part with respect to $(y, x; \Gamma^{-1})$. Moreover $\partial_-(X^\wedge) = \partial(X)$.*

In particular x is $(k-1)$ -nonseparable from y in Γ^{-1} , if y is $(k-1)$ -nonseparable from x in Γ .

Proof.

We have clearly $\partial_-(X^\wedge) \subset \partial(X)$. Put $C = \partial(X) \setminus \partial_-(X^\wedge)$.

Since $y \notin \Gamma(X \cup C)$, we have $k \leq |\partial(X \cup C)| \leq |\partial_-(X^\wedge)| \leq |\partial(X)| = k$.

■

The above lemma is a local version of the isoperimetric duality.

Lemma 14 *Assume that $\Gamma = (V, E)$ is k -critical and that $\Gamma(x) \cap \Gamma^{-1}(y) = \emptyset$. There is a k -part F of Γ such that $\min(|F|, |F^\wedge|) \geq 2$.*

Proof.

Take a path $[x, a, b, \dots, c, y]$ of minimal length from x to y . By Lemma 12, there is a k -part F , with $a \in F$ and $b \in \partial(F)$. We have $\{x, a\} \subset F$. We have $|F^\wedge| \geq 2$ since otherwise $F^\wedge = \{y\}$. Hence by Lemma 13, $b \in \partial(F) = \partial^-(\{y\})$. Therefore $b \in \Gamma(x) \cap \Gamma^{-1}(y)$, a contradiction.

■

Let x be an element of V and let $T = \{y_1, \dots, y_k\}$ be a subset of $V \setminus \{x\}$. A family of k -openly disjoint paths P_1, \dots, P_k , where P_i is a path from x to y_i will be called an (x, T) -fan.

Proof of Theorem 4:

The proof is by induction, the result being obvious for $|V|$ small. Assume first that there $z \in \Gamma(x) \cap \Gamma^{-1}(y)$. Consider the restriction Ψ of Γ to $V \setminus \{z\}$. Clearly y is $(k-2)$ -nonseparable

from x in Ψ . By the induction hypothesis there are $(k - 1)$ -openly disjoint paths from x to y in Ψ . We adjoin the path $[x, z, y]$ to these paths and we are done. So we may assume that $\Gamma(x) \cap \Gamma^{-1}(y) = \emptyset$.

By Lemma 14 there is a part F with $\min(|F|, |F^\wedge|) \geq 2$. Consider the reflexive graph $\Theta = (V', E')$ obtained by contracting F^\wedge to a single vertex y_0 . We have $V' = (V \setminus F^\wedge) \cup \{y_0\}$. Since $|V'| < |V|$, by the induction hypothesis there are k openly disjoint paths from x to y_0 . By deleting y_0 we obtain an $(x, \partial(F))$ -fan. Similarly by contracting F and applying induction, we form a $(\partial(F), y)$ -fan.

By composing these two fans, we form k openly disjoint paths from x to y . ■

Remerciement L’auteur tient à remercier Jean Claude Fournier pour des discussions stimulantes au tour du Théorème de Menger.

l’Auteur tient aussi à remercier Eric balandraud, David Grynkiewicz, Alain Plagne, Oriol Serra et Gilles Zémor pour d’autres discussions sur des problèmes additifs et isopérimétriques.

Ce manuscrit a été préparé lors d’un séjour en Mauritanie où l’auteur a pu bénéficier d’un climat favorable au travail dans les locaux du CFED Nouakchott. Je tiens donc remercier M. Isselmou O. Mohamed et l’ensemble son personnel.

References

- [1] E. Balandraud, Un nouveau point de vue isopérimétrique appliqué au théorème de Kneser, *Preprint*, december 2005.
- [2] A. Cauchy, Recherches sur les nombres, *J. Ecole polytechnique* 9(1813), 99-116.
- [3] H. Davenport, On the addition of residue classes, *J. London Math. Soc.* 10(1935), 30–32.
- [4] J. Dixmier, Proof of a conjecture by Erdős, Graham concerning the problem of Frobenius, *J. number Theory* 34 (1990), 198-209.
- [5] D. Grynkiewicz, Quasi-periodic decompositions and the Kemperman’s structure theorem, *European J. Combin.* 26 (2005), no. 5, 559–575.
- [6] D. Grynkiewicz, A step beyond Kemperman’s structure Theorem, *Preprint* May 2006.
- [7] Y.O. Hamidoune, Sur les atomes d’un graphe orienté, *C.R. Acad. Sc. Paris A* 284 (1977), 1253–1256.
- [8] Y.O. Hamidoune, Quelques problèmes de connexité dans les graphes orientés, *J. Comb. Theory* B 30 (1981), 1-10.
- [9] Y.O. Hamidoune, On the connectivity of Cayley digraphs, *Europ. J. Combinatorics*, 5 (1984), 309-312.
- [10] Y.O. Hamidoune, Subsets with small sums in abelian groups I: The Vosper property. *European J. Combin.* 18 (1997), no. 5, 541–556.

- [11] Y.O. Hamidoune, An isoperimetric method in additive theory. *J. Algebra* 179 (1996), no. 2, 622–630.
- [12] Y.O. Hamidoune, On small subset product in a group. Structure Theory of set-addition, *Astérisque* no. 258(1999), xiv-xv, 281–308.
- [13] Y.O. Hamidoune, Some results in Additive number Theory I: The critical pair Theory, *Acta Arith.* 96, no. 2(2000), 97-119.
- [14] Y.O. Hamidoune, Some additive applications of the isoperimetric approach, <http://arxiv.org/abs/math/07060635>.
- [15] Y. O. Hamidoune , A. Plagne. A new critical pair theorem applied to sum-free sets. *Comment. Math. Helv.* 79 (2004), no. 1, 183–207.
- [16] J. H. B. Kemperman, On small sumsets in Abelian groups, *Acta Math.* 103 (1960), 66–88.
- [17] V. F. Lev, Critical pairs in abelian groups and Kemperman’s structure theorem. *Int. J. Number Theory* 2 (2006), no. 3, 379–396.
- [18] H.B. Mann, *Addition Theorems*, R.E. Krieger, New York, 1976.
- [19] M. B. Nathanson, *Additive Number Theory. Inverse problems and the geometry of sum-sets*, Grad. Texts in Math. 165, Springer, 1996.
- [20] T. Tao, V.H. Vu, *Additive Combinatorics*, Cambridge Studies in Advanced Mathematics 105 (2006), Cambridge University Press.